AUDITORIA INTERNA - AI

SEÇÃO DE AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO E DE GOVERNANÇA - SATIG

RELATÓRIO DE AUDITORIA nº. 4/2024

PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

SÃO LUIS – MA, 2024.

PREÂMBULO

PROCESSO: SEI n. 0008122-62.2024.6.27.8000.

ATO ORIGINÁRIO: Plano de Auditoria de Longo Prazo (PALP) 2022 a 2025, aprovado pela Portaria TRE/MA n. 1.581/2021 (SEI n. 0009517-94.2021.6.27.8000) e Plano Anual de Auditoria (PAA) 2024, aprovado pela Portaria TRE/MA n. 1.851/2023 (SEI n. 0012596-13.2023.6.27.8000).

OBJETIVO: Avaliar a gestão de segurança da informação no âmbito do TRE-MA, de modo a certificar-se da conformidade e da adoção de programa de tratamento e gestão de resposta a incidentes, utilizando como critério principal o *framework CIS Controls* (*The Center for Internet Security*) versão 8.

ATO DE DESIGNAÇÃO: Memorando n. 1.069/2024 – TRE-MA/PR/AI, de 29/11/2024 (id. 1994942, SEI n. 0012596-13.2023.6.27.8000).

PERÍODO ABRANGIDO PELA AUDITORIA: maio/2024 a novembro/2024.

PERÍODO DE REALIZAÇÃO DA AUDITORIA: a) Planejamento – maio a junho/2024; b) Execução – julho a outubro/2024; e c) Relatório – novembro/2024.

UNIDADE AUDITADA: Secretaria de Tecnologia da Informação e Comunicação – STIC.

RESUMO

A presente auditoria tem como objeto avaliar, no âmbito do Tribunal Regional Eleitoral do Maranhão, a gestão de resposta a incidentes da organização, utilizando como critério o Controle 17 do *framework CIS Controls* versão 8, que se concentra na Resposta a Incidentes.

Em síntese, os objetivos desta ação de controle consubstanciaram-se em verificar a eficácia das práticas atuais e propor melhorias que garantam uma resposta adequada e eficiente a incidentes de segurança, avaliando se a organização possui um plano formal de resposta a incidentes; está preparada para lidar com uma possível crise cibernética; e, realiza análises pós-incidentes para prevenir futuros incidentes semelhantes.

Ao término dos trabalhos, a principal inconformidade identificada foi a ausência de planejamento e procedimentos de condução de exercícios de simulação e testes de resposta a incidentes rotineiros e cenários para preparar o pessoal-chave envolvido no processo para responder a incidentes no mundo real e para validação da política e planos existentes.

Os benefícios decorrentes da implementação das medidas corretivas propostas são qualitativos, correspondentes ao aperfeiçoamento da gestão e governança de TIC no que toca à segurança da informação.

LISTA DE ABREVIATURAS E SIGLAS

AI	Auditoria Interna
CIS	*The Center for Internet Security*
CNJ	Conselho Nacional de Justiça
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes computacionais
PAA	Plano Anual de Auditoria – TRE/MA
PALP	Plano de Auditoria de Longo Prazo – TRE/MA
PSI	Política de Segurança da Informação
PT	Papel de Trabalho
SATIG	Seção de Auditoria de Tecnologia da Informação e Comunicação e de Governança – TRE/MA
SEI	Sistema Eletrônico de Informações
STIC	Secretaria de Tecnologia da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação
TRE/MA	Tribunal Regional Eleitoral do Maranhão
TRT	Tribunal Regional do Trabalho
TSE	Tribunal Superior Eleitoral

SUMÁRIO

I. INTRODUÇÃO

1. A presente auditoria tem como objetivo avaliar a gestão de segurança da informação no âmbito do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com base nos critérios estabelecidos pelo *CIS Controls (The Center for Internet Security)*, versão 8, especificamente o Controle 17 - Gestão de Resposta a Incidentes. Este controle visa desenvolver e manter uma capacidade de resposta a incidentes por meio de políticas, planos, procedimentos, funções definidas, treinamentos e comunicações, preparando a organização para detectar e responder rapidamente a ataques.

2. A gestão de segurança da informação é um processo fundamental para proteger os ativos de informação contra ameaças diversas, garantindo a confidencialidade, integridade e disponibilidade dos dados. Em um cenário cada vez mais digital e conectado, a capacidade de identificar e responder a incidentes de segurança de maneira eficiente e eficaz torna-se crucial. A ausência de uma gestão robusta pode levar a perdas significativas de dados, interrupções de serviço e impactos financeiros e reputacionais negativos.

3. O Controle 17 do *CIS Controls* versão 8 enfatiza a importância de uma abordagem estruturada para a resposta a incidentes. Isso inclui o desenvolvimento de políticas e planos detalhados, a realização de exercícios de simulação e testes de resposta a incidentes, e a capacitação contínua do pessoal-chave. Essas práticas não apenas melhoram a prontidão da organização para enfrentar incidentes, mas também permitem a validação e o aprimoramento contínuo das políticas e procedimentos de segurança.

4. Dessa forma, a auditoria visa certificar-se da conformidade do TRE-MA com os requisitos do Controle 17, identificando áreas de melhoria e recomendando ações para fortalecer a postura de segurança da informação da instituição.

5. Cabe destacar a atuação consonante desta Seção de Auditoria de Tecnologia da Informação e Comunicação e de Governança – SATIG, em cumprimento ao estabelecido no Plano de Auditoria de Longo Prazo (PALP) 2022 a 2025, aprovado pela Portaria TRE/MA n. 1.581/2021 (SEI n. 0009517-94.2021.6.27.8000) e Plano Anual de Auditoria (PAA) 2024, aprovado pela Portaria TRE/MA n. 1.851/2023 (SEI n. 0012596-13.2023.6.27.8000), realizando exames de auditoria no processo de gestão de segurança da informação.

6. Neste contexto, a presente auditoria apoiou-se no Plano de Trabalho n. 01/2024 (id. 2151185, SEI n. 0008122-62.2024.6.27.8000) estabelecido pela SATIG.

7. Compuseram a equipe de auditoria a servidora Sara Aguiar Gomes (matrícula 3099950) e o servidor Moisés Dantas Linhares (matrícula 30990117).

8. O possível achado encontrado e as respectivas recomendações emitidas por esta unidade foram materializados no Quadro de Achados (id. 2344131, SEI n. 0008122-62.2024.6.27.8000) e encaminhados para a unidade auditada.

9. A unidade auditada se manifestou quanto ao possível achado, e suas respostas foram consideradas e incluídas neste Relatório de Auditoria.

10. Todos os exames realizados se pautaram em procedimentos e técnicas de auditoria aplicáveis à Administração Pública e nenhuma restrição foi imposta quanto ao método ou à extensão dos trabalhos realizados.

II. VISÃO GERAL DO OBJETO AUDITADO

11. O objeto auditado nesta análise é o processo de gestão de segurança da informação do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com foco específico no Controle 17 - Gestão de Resposta a Incidentes, conforme estabelecido pelo *framework CIS Controls (The Center for Internet Security)*, versão 8. Este controle é fundamental para garantir que a organização esteja preparada para responder de maneira eficiente e eficaz a incidentes de segurança, minimizando os impactos adversos e assegurando a continuidade das operações.

12. Um programa de segurança cibernética deve incluir proteção, detecção, resposta e recuperação. Muitas instituições negligenciam resposta e recuperação, optando por restaurar sistemas comprometidos, sem abordar as causas. A resposta a incidentes visa identificar, responder e remediar ameaças antes que causem danos. Sem um entendimento completo de um incidente, as defesas se tornam ineficazes.

13. A equipe de resposta deve treinar periodicamente com cenários ajustados às ameaças que a instituição enfrenta, garantindo que todos entendam suas funções e identificando lacunas nos planos. O Controle CIS 17 oferece etapas prioritárias que melhoram a segurança e devem integrar qualquer plano abrangente de resposta a incidentes.

14. Através desta auditoria, buscamos identificar áreas de melhoria e recomendar ações que possam aprimorar a capacidade do TRE-MA em responder a incidentes de

segurança de forma eficaz, assegurando uma gestão de segurança da informação sólida e confiável.

15. Esta visão geral oferece um contexto abrangente para a leitura do relatório, destacando o processo de gestão de segurança da informação do TRE-MA. A análise detalhada subsequente abordará as conclusões da auditoria e fornecerá recomendações práticas para aprimorar ainda mais a capacidade do TRE-MA em responder a incidentes de segurança de maneira eficiente e eficaz.

III. OBJETIVO DA AUDITORIA

16. Este trabalho de auditoria tem como objetivo avaliar a gestão de segurança da informação no âmbito do TRE-MA, de modo a certificar-se da conformidade e da adoção de programa de tratamento e gestão de resposta a incidentes, utilizando como critério principal o *framework CIS Controls* (*The Center for Internet Security*) versão 8.

IV. QUESTÕES DA AUDITORIA

17. Os testes para a realização desta auditoria foram elaborados pela SATIG a partir das seguintes questões de auditoria, conforme tabela abaixo:

Questões de Auditoria
Q1. A organização possui um plano formal de resposta a incidentes?
Q2. A organização está preparada para lidar com uma possível crise cibernética?
Q3. A organização realiza análises pós-incidentes para prevenir futuros incidentes semelhantes?

V. ESCOPO

18. O escopo é importante para direcionar os trabalhos e dar conhecimento mais abrangente da auditoria para a Alta Administração e para a unidade auditada.

19. A necessidade de se proteger dados é premente na sociedade moderna. Para os órgãos da Administração Pública, que se utilizam de inúmeros relacionamentos com colaboradores, empresas e prestadores de serviço para a consecução de suas atividades, a segurança da informação se torna fundamental.

20. Diante disso, selecionou-se como objeto de avaliação para esta auditoria o Controle 17 do *The Center for Internet Security* (*CIS Controls*) versão 8, denominado Gestão de Resposta a Incidentes. Segundo o CIS, esse é um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.

VI. CRITÉRIOS

21. Os critérios utilizados como parâmetros para fundamentar as avaliações apresentadas neste trabalho foram:

a) *CIS Controls Framework* – Versão 8 (Maio/2021);

b) Resolução CNJ n. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

c) Resolução TSE n. 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

d) Portaria CNJ n. 162/2021, que trata sobre Protocolos e Manuais criados pela Resolução CNJ n. 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

e) Decreto n. 9.637/2018, que Institui a Política Nacional de Segurança da Informação;

f) Portaria TRE-MA n. 101/2024, que atualiza o processo de gerenciamento de incidentes no âmbito da Secretaria de Tecnologia da Informação e Comunicação;

g) Portaria TRE-MA n. 939/2022, que cria a Equipe de Tratamento e Resposta a Incidentes em Redes computacionais (ETIR) da Justiça Eleitoral do Maranhão e disciplina suas atividades;

h) Portaria TRE-MA n. 143/2022, que institui o Comitê de Crise Cibernética e define a sala de situação;

i) Portaria TRE-MA n. 1647/2021, que estabelece nova composição da Comissão de Segurança da Informação e complementa as suas atribuições;

j) Instrução Normativa TRE-MA n. 6/2022, que dispõe sobre regras e procedimentos empregados pela Equipe de Tratamento e Resposta a Incidentes em Redes computacionais da Justiça Eleitoral do Maranhão;

k) Plano de Conscientização e Treinamento em Segurança da Informação e Comunicação 2022 - TRT 16ª Região. Disponível em: https://www.trt16.jus.br/governanca-institucional/governanca-de-tic/planos-de-tic (Planos de TIC | Portal do TRT 16ª Região - Maranhão).

VII. ACHADOS DE AUDITORIA

22. Os achados representam o resultado dos testes de auditoria aplicados e das informações coletadas nas entrevistas, questionários, análises documentais e correlação de informações conforme Programa de Auditoria.

23. Após a realização dos testes, e com base nas informações respondidas pela área de Tecnologia da Informação, chegou-se às seguintes conclusões apresentadas abaixo:

ACHADO 1: AUSÊNCIA DE PLANEJAMENTO E PROCEDIMENTOS DE CONDUÇÃO DE EXERCÍCIOS DE SIMULAÇÃO E TESTES DE RESPOSTA A INCIDENTES ROTINEIROS E CENÁRIOS PARA PREPARAR O PESSOAL-CHAVE ENVOLVIDO NO PROCESSO PARA RESPONDER A INCIDENTES NO MUNDO REAL E PARA VALIDAÇÃO DA POLÍTICA E PLANOS EXISTENTES.

24. **Situação encontrada:** Conforme resposta ao questionário e correlação entre as informações obtidas, constatou-se que não há planejamento, nem procedimentos de exercícios de simulação e testes de resposta a incidentes rotineiros e cenários para preparar o pessoal-chave envolvido no processo para responder a incidentes no mundo real e para validação da política e planos. Os exercícios precisam testar os

canais de comunicação, tomada de decisão e fluxos de trabalho, e ser realizados anualmente, no mínimo.

25. **Critérios de auditoria:**

- *CIS Controls Framework* - Versão 8 - Controle 17, Medida de Segurança 17.7;
- Resolução CNJ n. 396/2021, art. 11, I, III, X e XI, art. 19, IV e VI;
- Portaria CNJ n. 162/2021, Anexo II - Protocolo - Gerenciamento de Crises Cibernéticas do Poder Judiciário, subitem 4.1, "f" e "g"; e Anexo V - Manual de referência - Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, itens 28,"a" e "b", 33, "i" e "q".

26. **Evidências:**

- PT.E.2.0 – Formulário 2 (Questões 1 e 2).

27. **Possíveis causas:**

- Possível deficiência nos controles internos da(s) unidade(s) responsável(is) pelo planejamento, tratamento e respostas a incidentes de segurança;
- Não adoção de boas práticas de Segurança da Informação estabelecidas na medida de segurança 17.7 do controle 17 do *CIS Controls* - versão 8.

28. **Consequências do achado:**

- Risco potencial à capacidade de resposta a incidentes de segurança reais, comprometendo a melhoria contínua da postura de segurança;
- Risco potencial de impacto na continuidade das atividades essenciais do TRE-MA, incluindo perda de dados e interrupção de serviços.
- Risco potencial de impacto na imagem e reputação da instituição;
- Potencial comprometimento da confidencialidade, integridade e disponibilidade das informações da Justiça Eleitoral;
- Potencial exposição indevida de informações, sistemas e processos críticos da organização.

29. **Manifestação da unidade auditada sobre o achado:**

- Despacho n. 91315/2024 – TRE-MA/PR/DG/STIC/SESEC (id. 2345326, SEI n. 0008122-62.2024.6.27.8000): “Em atenção ao Memorando nº 1385/2024 - TRE-

MA/PR/AI/SATIG (doc. 2344088), informamos nossa concordância com o Item A1 da Matriz de achados e com a recomendação."

30. **Análise sobre a manifestação da unidade auditada:** A unidade auditada corrobora o achado, motivo pelo qual apresentamos a proposta de encaminhamento a seguir.

31. **Proposta de encaminhamento:** Ante o exposto, recomenda-se:

À Secretaria de Tecnologia da Informação e Comunicação (STIC), a implementação de Planejamento e Procedimentos de condução periódica de Exercícios de Simulação e Testes de Resposta a Incidentes, bem como a utilização dos relatórios destes exercícios para melhorar e ajustar a política e os planos existentes.

32. **Conclusão:** A manifestação da unidade auditada corrobora o achado de auditoria e a recomendação apresentada no Quadro de Achados (id. 2344131, SEI n. 0008122-62.2024.6.27.8000), razão pela qual mantém-se a proposta de encaminhamento constante no item 31 deste Relatório.

VIII. CONCLUSÃO

33. No cenário mundial, as informações são um dos ativos organizacionais mais valiosos e, portanto, protegê-las adequadamente de ameaças digitais tornou-se meta essencial para garantir a sobrevivência e a confiança da sociedade na continuidade dos serviços prestados. A Gestão de Resposta a Incidentes faz parte de um conjunto abrangente de práticas, políticas e controles planejados para proteger as informações contra ameaças cibernéticas, acesso não autorizado, vazamento de dados confidenciais, uso indevido e outras formas de violação digital.

34. Além disso, a Gestão de Resposta a Incidentes é tida como medida essencial em um sistema de proteção organizacional, pois sabe-se que, em termos de segurança da informação e segurança cibernética, não existem sistemas ou organizações 100% seguros. Portanto, para que sistemas, serviços e processos possam ter maior resiliência e resistir a eventos de risco, contar com mecanismos eficientes de identificação e de resposta a incidentes é parte fundamental para o sucesso na proteção organizacional.

35. Esta auditoria interna teve como objetivo avaliar a gestão de segurança da informação no âmbito do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com base nos critérios estabelecidos pelo *CIS Controls (The Center for Internet Security)*, versão 8,

especificamente o Controle 17 - Gestão de Resposta a Incidentes. Este controle visa desenvolver e manter uma capacidade de resposta a incidentes por meio de políticas, planos, procedimentos, funções definidas, treinamentos e comunicações, preparando a organização para detectar e responder rapidamente a ataques.

36. No tocante à implementação do controle 17 do *CIS Controls* v8 - Desenvolvimento e implementação de uma infraestrutura de resposta a incidentes, verificou-se que o Tribunal, embora tenha estabelecido práticas significativas para gestão de resposta a incidentes, apresenta uma necessidade crítica de implementar exercícios regulares de simulação (Medida de Segurança 17.7). Esses exercícios são essenciais para validar os planos existentes, treinar as equipes envolvidas e garantir que todos os canais de comunicação estejam funcionando adequadamente durante um incidente real.

IX. PROPOSTAS DE RECOMENDAÇÃO

37. Diante do exposto, submete-se o presente relatório à consideração do Dirigente da Auditoria Interna (AI), para posterior encaminhamento ao Exmo. Presidente deste Egrégio Tribunal, destacando a recomendação sugerida à Secretaria de Tecnologia da Informação e Comunicação (STIC), conforme detalhamento a seguir:

38. Recomendar que a STIC implemente Planejamento e Procedimentos de condução periódica de Exercícios de Simulação e Testes de Resposta a Incidentes, bem como a utilização dos relatórios destes exercícios para melhorar e ajustar a política e os planos existentes.

É o Relatório.

São Luís/MA, 4 de dezembro de 2024.

gov.br Documento assinado digitalmente
MOISES DANTAS LINHARES
Data: 04/12/2024 09:59:31-0300
Verifique em https://validar.iti.gov.br

Moisés Dantas Linhares

Auditor interno
Técnico Judiciário - matrícula 30990117

gov.br Documento assinado digitalmente
SARA AGUIAR GOMES
Data: 04/12/2024 10:03:11-0300
Verifique em https://validar.iti.gov.br

Sara Aguiar Gomes

Auditora interna
Técnico Judiciário - matrícula 3099950
Chefe da SATIG